Notice of Allowability	Application No.	Applicant(s)	
	09/727,300	POMET ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *6 August 2007*.

2. ☒ The allowed claim(s) is/are *12-49*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

1. This is in response to the arguments filed on 6 August 2007.

2. Claims 12-49 are pending in the application.

3. Claims 12-49 have been allowed.

4. Claims 1-11 have been cancelled.

Response to Arguments

5. Applicant's arguments, see pages 13-18, filed 6 August 2007, with respect to claims 12-49 have been fully considered and are persuasive. The rejection of the claims has been withdrawn.

Allowable Subject Matter

6. Claims 12-49 are allowed.

The following is an examiner's statement of reasons for allowance:

The current application, as recited in independent claim 12, for example, is directed towards an electronic device comprising a central processing unit, at least one peripheral device, and a data bus connected between the at least one peripheral device and the central processing unit through which data travels at a rate of a clock signal. The electronic device further comprises a transmission line connected between the at least one peripheral device and the central processing unit for providing a random signal thereto that is synchronous with the clock signal. The central processing unit and the at least one peripheral device each comprises a data encryption/decryption cell connected to the data bus and to the transmission line for generating a same current secret key at each clock cycle based upon the random signal. The electronic device is advantageously secure since the transmission line is separate from the data bus, yet both are connected between the at least one peripheral device and the central processing unit. Moreover, the data

encryption/decryption cell in the central processing unit and in the at least one peripheral device advantageously makes the electronic device more secure by making it more difficult to determine the data elements that travel through the data bus when an intruder observes current consumption of the electronic device. Independent device claim 25 is similar to independent device claim 12 except the at least one peripheral device has been changed to at least one memory device. Independent device claim 34 is similar to independent device claim 12 except this claim is directed to a smart card. Independent method claim 42 is similar to independent device Claim 12.

The closest prior art to the current application was Carmeli U.S. Patent No. 6,865,672 (hereinafter Carmeli). The Carmeli patent discloses a system for providing a trusted computer communication network including a master decision maker unit coupled to the trusted network, and at least one slave communication unit coupled to the master unit by a wide bus connection that has multiple unidirectional communication channels, and connected to a non-trusted network. The trusted network is physically isolated at all times from the non-trusted network, and all data transported between the trusted network and the non-trusted network is transported between the master unit and the slave unit.

However, there are differences between the current application and the Carmeli patent. The transmission lines 30 and 32 of Carmeli are separate from each other. As a result, there is no transmission line connected between the master unit 36 and the slave unit 34. However, there is a data bus 38 connected between the master unit 36 and the slave unit 34. The data bus 38 is a non-supported high-speed bus, which consists of essentially any connection bus having several unidirectional data channels or communication lines that connect two wide bus gate cards. The transmission line in the current application, which is connected between the processor and the at least one peripheral device, provides a synchronous random signal to the processor and the peripheral device, and from which each one produces locally the same value of the secret

key, wherein the secret key is used to secure data exchanges between them. In the Carmeli patent, transmission lines 30 is connected to a hostile network, whereas transmission line 32 is connected to a trusted network. Since these two networks are separate from one another, transmission lines 30 and 32 are also separate from one another. As recited in the claims of the current application, the data bus and the transmission line are separated from one another, as best shown in FIG. 2 in the Applicants' application. Carmeli fails to provide this noted distinction. Reference is directed to column 7, lines 52 to 63 of Carmeli, which provides: "The standard computer communication network, whether it is the hostile or the trusted net, is always connected to the SBC. Units exchange data through the wide bus gate card, and only through these sections. The internal communication between the SBC and the wide bus gate cards is done through a standard computer 28 (shown in FIG. 3), which may be, for example, a PCI or ISA bus. The SSC can freely write data to the wide bus gate card, but does not have direct access to the wide bus." No transmission line, distinct from the computer bus 28, can be identified in the slave or master unit of Carmeli between the BBC 22 and the wide bus gate card **24,** which could be used to provide a synchronous random signal to each section 22 and 24 or the master or slave unit for the production of the common secret key. In addition, Carmeli teaches that the random values used to produce the secret key are generated by the wide bus gate card **24** at the time of starting, and that these values are transmitted on the computer bus 28 to the SBC 22. Reference is directed to column 9, lines 32 to 42 of Carmeli, which provides: "The permanent values are randomly generated by the wide bus gate card at startup time. Since, at that time, the system (i.e., the hardware described above) is physically disconnected from both networks, it is safe to send these values to the SBC through the computer bus. In addition, the wide bus gate card generates another number that is considered as the current secret key number, and it sends that number to the SBC, right after the permanent values. Now, both sections are synchronized; both use the same function (because they use the same permanent values) and both start from the same initial value of a secret key." Consequently, the two sections 22 and 24 are

synchronized and can produce the same secret key starting from these exchanged random values. Carmeli fails to disclose a transmission line distinct from the bus 28 that is used to transmit a synchronous random signal to each section 22, 24, from which the common secret key would be produced. On the contrary, the random values used to produce the secret key common to each section are transmitted on the computer bus at the time of starting. Furthermore, according to the current application, the processor and the peripheral device locally produce a current value of the secret key at each cycle of clock from the random signal synchronous of the clock signal. In sharp contrast, Carmeli discloses the current value of the secret key is modified on randomly generated request (column 9, lines 50-53). The modification of the current value of the secret key is thus not controlled by the clock signal contrary to the claimed invention.

For the reasons stated above, it is submitted that independent claim 12 is patentable over prior art. Independent claims 25, 34 and 42 are similar to independent Claim 12. It is submitted that these independent claims are also patentable over prior art.

Any claims not directly addressed are allowed on their virtue of dependency.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Aravind K Moorthy
August 21, 2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100